LISTING OF THE CLAIMS:

The following is a complete listing of all the claims in the application, with an indication of the status of each:

1-3. (Canceled).

4. (Previously Presented) A method of verifying knowledge of a secret number s in a prover device by a verifier device having no knowledge of the secret number, the method comprising a zero-knowledge protocol using a Montgomery representation of numbers and Montgomery multiplication operations therein,

wherein the zero knowledge protocol comprises the Fiat-Shamir protocol,

the method further comprising:

(i) providing to the verifier device a value $v = s^2$ being the Montgomery multiplication of the secret number s by itself,

(ii) computing, by the prover device, a value $x = \mathrm{r}\, x_{\mathrm{m}}\, r$, where r is a random number, and transmitting the value x to the verifier device;

(iii) selecting, by the verifier device, a challenge value of e from a set {0, 1} and transmitting the challenge value to the prover device;

(iv) computing, by the prover device, a value $y = r\, x_{\mathrm{m}}\, s^e$, and transmitting the value y to the verifier device; and

(v) the verifier device checking an authenticity of the prover's response according to the values x, y and v previously received and according to the challenge value e.

5. (Previously Presented) The method of claim 4 wherein the step of checking the authenticity of the prover's response comprises the steps of:

for a challenge value of $e = 1$, computing the values of $y\ x_m y$ and $v\ x_m x$ and checking that they are the same; or

for a challenge value of $e = 0$, computing the value of $y\ x_m y$ and checking that it is the same as the previously received value of x.

6. (Previously Presented) The method of claim 4 further including the steps of repeating steps (ii) to (v) for a number of consecutive rounds to confirm the authenticity of the prover's response.

7. (Previously Presented) The method of claim 4 in which the secret number s is a Montgomery representation of another number s' known in the prover device domain but not in the verifier device domain, further including the step of computing, by the prover device, the value of s from s' according to $\underline{s} = s'R \bmod n$, where $R>n$, values of n and R being used by both the prover device and the verifier device.

8. (Previously Presented) The method of claim 4 in which the Montgomery multiplications of $s\ x_m\ s$, $r\ x_m\ r$, and $r\ x_m\ s^e$ are carried out according to the formula $a\ x_m\ b = abR^{-1} \bmod n$, where $R>n$, values of n and R being used by both the prover device and the verifier device.

9. (Previously Presented) The method of claim 5 in which the Montgomery multiplications of $y\ x_m\ y$ and $s^2\ x_m\ x$ are carried out according to the formula $a\ x_m\ b = abR^{-1} \bmod n$, where $R>n$, values of n and R being used by both the prover device and the verifier device.

10. (Previously Presented) The method of claim 4 in which all computations in the zero knowledge protocol are performed using Montgomery representation of numbers and using Montgomery multiplication operations.

11 - 30. (Canceled)